UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,481	07/23/2003	Makoto Fujiwara	60188-593	7409

7590 10/28/2008

Jack Q. Lever, Jr.
McDERMOTT, WILL & EMERY
600 Thirteenth Street, N.W.
Washington, DC 20005-3096

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
10/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/624,481	FUJIWARA ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *9 and 11* is/are allowed.

6)☒ Claim(s) *1-8 and 10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *08/08 & 06/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on July 16, 2008. Independent claims 1, 8-11 are amended. Claims 1-11 are pending/examined.

Priority

2. Receipt is acknowledged of papers submitted Under 35 U.S.C. 119 (a)-(d), which papers have been placed of record in the file.

3. In the previous office action **claims 9 and 11** were objected to as being dependent upon a rejected base claim, but indicated that they would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Accordingly, applicant's representative have rewritten claims 9 and 11 into independent form. Thus the objection made to claims 9 and 11 is withdrawn and claims 9 and 11 are allowed.

Response to Argument

4. Applicant's remark/arguments filed on July 16, 2008 have been fully considered but they are not persuasive.

Referring to the amended Independent claim 1, Applicant's representative argued that the reference/s on the record, namely Lin does not disclose/teach the following amended underlined limitation recited as "setting the provided LSI device to a development mode **based on an inherent key information, which is implemented in the LSI device in advance..."**

Referring to the amended Independent claims 8 and 10, Applicant's representative argued that the reference/s on the record namely Lin does not disclose/teach the following amended underlined limitation recited as the development LSI device includes a secure memory for storing **encrypted** common key information regarding a raw common key, **which is implemented in the LSI device in advance..."**

Applicant's representative wrote the following in support of the above argument.

"It is respectfully submitted that Lin is completely silent as to such a feature.

In direct contrast, Lin expressly discloses accessing a public key rather than one which is implemented in the alleged LSI device 104 in advance. Indeed, Lin discloses at paragraph 12 (emphasis added):

To facilitate security operations in the mobile communication device 104, a public key infrastructure service provider has a machine or server 118 operatively coupled to the Internet, and is such that other machines operatively coupled to the Internet can transact with the server 118. Generally, such service providers provide encryption technologies such as public keys and authentication services including digital encryption

certificates and code signing services for use by software and code developers. Such products and services are used by target devices to verify the authenticity of software and code obtained over public networks."

Examiner disagrees with the above argument.

Examiner would like to point that the feature that the applicant's is arguing is already disclosed by the reference on the record.

In particular Lin on paragraph 0016 and 0017 and claim 1 discloses the following.

The present invention accomplishes this by use of a new class of certificate referred to as a development certificate. The development certificate specifies the machine it is to be used with, such as by specifying the international mobile equipment identifier of a mobile communication device, for example, and specifying a development parameter. The development parameter can specify the time period of use, the number of uses, and so on. Using the newly developed type of certificate, a developer can specify the particular mobile communication device on which the code is to be tested, obtain a development certificate from a public key infrastructure provider such as a certificate authority, **and test several versions of the code being developed, on a live system, with device which has the same security environment as one sold into retail channels**.[Paragraph 0009]

On paragraph 0017-0018 Lin, the reference on the record discloses following.

"The mobile communication device also creates and stores a hash of the development parameter (338) for use with subsequently loaded versions of the software. This hash is stored in non volatile memory. The security permissions are then set according to the descriptor file 206, and the application can then be installed. The development parameter used is a number of times the code may be executed, each time the code is called, it will increment a count of the number of times it has been called, keep this count in a cryptographically secure format in the mobile communication device's non-volatile memory, and check it each time the software is called to determine if the software can still be used. The same is true for other development parameters that may be used such as validity period, for example. Each time the software is called, the development parameters are checked against the present condition of those parameters to determine if the development certificate is still valid. If not, then execution of the software is immediately aborted. Therefore, execution of the software commences only if the device identifier of the development certificate matches the device identifier of the portable device or mobile communication device, and the development parameter is likewise valid."

Therefore Examiner would like to point out that, unlike to the applicant's argument, this development parameter (338) and the device identifier which are met to be "inherent key information/common key information" are pre-stored/implemented on the target mobile device; And contrary to

the applicant's argument these parameters are implemented in the LSI device in advance.

Thus as it is disclosed above, each time the software is called by the LSI device or when the Software is loaded on the LSI device, the development parameters are checked against the present condition of those parameters which are already pre-installed/implemented in the LSI device to determine if the development certificate is still valid. If not, then execution of the software on the LSI device is immediately aborted. Therefore, execution of the software on LSI device commences only if the device identifier of the development certificate matches the **device identifier of the portable device or mobile communication device, and the development parameter which are already pre-installed in the LSI device in advance is likewise valid.**

Thus each and every amended independent claim is disclosed by the reference on the record. Thus the rejection is maintained.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the

invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

6. **Claims 1-8 and 10** are rejected under 35 U.S.C. 102(e) as being anticipated by Lin et al (hereinafter referred as Lin)(U.S. Publication No. 2002/0078380 A1) (filed on 12/20/2000).

7. As per independent claims 1 and dependent claim 2 Lin discloses a method for developing a program which is to be installed in a system having an LSI device [figure 1, ref. Num "104"], **the LSI device having a secure memory which includes an unrewritable area** [paragraph 0008] , **the method comprising the steps of:**

providing another LSI device having the same structure as that of the LSI device [Figure 1, ref. Num "108" and paragraph 0009]; **setting the provided LSI device to a development mode based on an inherent key information which is implemented in the LSI device in advance**[*See paragraph 0017-0018 the inherent key information which is met to be "the development parameter (338)" and "device identifier information" are stored/implemented in advance in every LSI device. See for instance "stores a hash of the development parameter (338) for use with subsequently loaded versions of the software. This hash is stored in non volatile memory on the LSI device and see also the device identifier which is already implemented/stored in every mobile device in advance.*

See also how using these inherent key information, the software is authenticated before it is executed on LSI device] **so that the provided LSI device is used as a development LSI device, the development mode being different from a product operation mode employed at the times of program installation and product operation; and developing the program on the development LSI device.** [Abstract, paragraph 0014 and paragraph 0016-0018 and claim 1]

8. **As per independent claims 8 and 10 Lin discloses a program development supporting system for supporting development of an encrypted program,***[Paragraph 0012]* **Comprising**

a development LSI device having the same structure as that of an LSI device on which the encrypted program runs *[Paragraph 0012]***; and**

an external memory for storing a raw (binary) program, wherein the development LSI device includes a secure memory for storing encrypted common key information regarding a raw common key which is implemented in the LSI device in advance, *[See paragraph 0017-0018 the common key information regarding a raw common key which is met to be "the development parameter (338)" and "device identifier information" are stored/implemented in advance in every LSI device. See for instance "stores a hash of the development parameter (338), which meets the limitation of "encrypted common key information" for use with subsequently loaded versions of the software. This hash is stored in non volatile memory on the LSI device and see*

also the device identifier which is already implemented/stored in every mobile device in advance. See also how using these encrypted common key information, the software is authenticated before it is executed on LSI device**] and the development LSI device is capable of executing a first step of obtaining the raw common key from the common key information stored in the secure memory, and a second step of encrypting the raw (binary) program input from the external memory using the raw common key.** *[Paragraph 0016-0017]*

9. **As per dependent claims 3 Lin discloses a method as applied to claims above. Furthermore Lin discloses the method further comprising the step of encrypting the program developed on the development LSI device at the program development step.** *[Paragraph 0012 and 0017]*

10. **As per dependent claims 4 Lin discloses a method as applied to claims above. Furthermore Lin discloses the method wherein the operation of the LSI device is restricted such that when being set to the development mode, the LSI device cannot generate a key for encrypting a raw (binary) program.** *[Paragraph 0016-0017]*

11. **As per dependent claims 5-7 Lin discloses a method as applied to claims above. Furthermore Lin discloses the method further comprising the steps of.' providing an LSI device having the same structure as that of the LSI device; setting the provided LSI device**

to a key-generation mode so that the provided LSI device is used as an key-generation LSI device, the key-generation mode being different from the development mode and the product operation mode; and installing an encrypted key-generation program in the key-generation LSI device and executing the key-generation program to generate a key.[Paragraph 0012 and 0016-0018 and claim 1]

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached

on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

10/15/2008

/Samson B Lemma/

Examiner, Art Unit 2432

/Gilberto Barron Jr/

Supervisory Patent Examiner, Art Unit 2432